

**Notice of References Cited**

Application/Control No.

10/523,840

Applicant(s)/Patent Under  
Reexamination  
BILLET ET AL.

Examiner

Matthew B. Smithers

Art Unit

2437

Page 1 of 2

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2004/0247114	12-2004	Joye, Marc	380/028
*	B	US-6,778,666	08-2004	Kuzmich et al.	380/28
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Liardet et al., "Preventing SPA/DPA in ECC Systems Using the Jacobi Form", 2001, Springer-Verlag, pp.391-401.
	V	Hisil et al., "Faster Group Operations on Elliptic Curves", Jan. 2009, Australasian Information Security Conference", pp.1-19.
	W	Macleod, "14-term Arithmetic Progressions on Quartic Elliptic Curves", 2006, Journal of Integer Sequences, Vol. 9, pp.1-4.
	X	Hisil et al., "New Formulae for Efficient elliptic Curve Arithmetic", 2007, Springer-Verlag, pp. 138-151.

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

**Notice of References Cited**

Application/Control No.

10/523,840

Applicant(s)/Patent Under  
Reexamination  
BILLET ET AL.

Examiner

Matthew B. Smithers

Art Unit

2437

Page 2 of 2

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Girard, "The Group of Weierstrass Points of a Plane Quartic with at Least Eight Hyperflexes", July 2006, pp. 1561-1583.
	V	
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.